Available online at www.sciencedirect.com
SCIENCE DIRECT®
Journal of Algebra 274 (2004) 164–191
JOURNAL OF Algebra
www.elsevier.com/locate/jalgebra

The plus closure of an ideal

Leslie D. Hayes

Department of Mathematics and Computer Science, Saint Joseph's University, 5600 City Avenue, Philadelphia, PA 19131, USA

Received 27 January 2003

Communicated by Craig Huneke

Abstract

If R is a local integral domain let R^+ denote the integral closure of R in an algebraic closure of its quotient field. If $z \in R^+$, we would like to understand the conditions under which $z \in IR^+$, where I is an ideal of R. Necessary and sufficient conditions on the coefficients of the minimal irreducible polynomial for z are known when I is generated by two elements of a regular system of parameters and when z is in a degree two extension of R. In this article we obtain results for the case when $z^3 \in R$, as well as a sufficient condition for z to be in IR^+ when $z^a \in R$ for $a \geqslant 1$ and I has a finite number of generators.

1. Introduction

Let R be an integral domain and I an ideal of R. The plus closure of I, denoted I^+, is defined to be $IR^+ \cap R$, where R^+ is the integral closure of R in an algebraic closure of its quotient field. Since $I^+ = \bigcap (IR_P)^+$ [1, p. 691] where the intersection is taken over all prime ideals P, we may restrict our attention to local integral domains, of which there are three types: those which contain the rationals (equicharacteristic 0), those which contain finite fields (equicharacteristic p), and those which do not contain a field (mixed characteristic).

If R is integrally closed and contains the rationals, then it is well known that $IS \cap R = I$ for any integral extension S of R. Hence $I^+ = I$. In the equicharacteristic p case, $I^+ \subseteq I^*$, where I^* denotes the tight closure of I, and it is conjectured that equality holds. As noted

E-mail address: lhayes@sju.edu.

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2003.08.014

above, the plus closure is a local property, so understanding it may help solve the primary problem in tight closure theory: does $I = I^*$ imply that $I_P = I_P^*$ for all prime ideals P?

In the mixed characteristic case, little is known about the plus closure. A 30-year old conjecture known as the monomial conjecture is actually an assertion that certain elements are not in the plus closures of certain ideals in regular local rings. Understanding the plus closure would also allow us to determine if R^+ is Cohen–Macaulay in dimension 3.

The question on which we will focus is the following: if I is an ideal in a regular local ring R and $z \in R^+$, when is $z \in IR^+$? Heitmann [2] has answered this question in the case where z satisfies a degree two polynomial $f(T) = T^2 + c_1T + c_2$ over R and $I = (x, y)R$, where x, y are part of a regular system of parameters for R. Letting $\Delta = (c_1)^2 - 4c_2$ denote the discriminant of f, his main result is the following.

Theorem 1. *Let R be a regular local ring, x, y part of a regular system of parameters, and $p \in (x, y)R$ with $p > 5$. Then $z \in IR^+$ if and only if $c_1 \in I$ and either*

(1) $\Delta \in t^2R$ *for some* $t \in I$,
(2) $\Delta \in I^4$, *or*
(3) $\Delta \in (t, I^2)^3R$ *for some* $t \in I$.

Notice that if $z^2 \in R$, then (1)–(3) become $z^2 \in t^2R$, $z^2 \in I^4$, and $z^2 \in (t, I^2)^3R$, respectively. If $z^3 \in R$, we make the following conjecture.

Conjecture 2. *Let R be a regular local ring and let x, y be part of a regular system of parameters for R. Suppose that p is a sufficiently large prime number and $p \in I = (x, y)R$. Let $z \in R^+$ such that $z^3 \in R$. Then $z \in IR^+$ if and only if one of the following holds*:

(1) $z^3 \in t^3R$ *for some* $t \in I$;
(2) $z^3 \in I^6$;
(3) $z^3 \in (t, I^3)^4$, $(t, I^2)^5$, *or* (t^5, I^8) *for some* $t \in I$.

The reverse implication is given as Corollary 19 in Section 3. The progress made toward the forward direction is discussed in Section 4. In particular, Proposition 26 shows that if (1) does not hold, then $z^3 \in t^4R + I^5R$ for some $t \in I$. Theorems 28, 32, and 35 then eliminate most of the remaining cases when $z^3 \notin I^5$.

In Section 3, Corollary 17 provides a sufficient condition for $z \in IR^+$ when $z^a \in R$, $a \geqslant 1$, and I is an ideal having a finite number of generators.

2. Preliminary results

All rings are assumed to be integral domains. Throughout this paper, $\lfloor x \rfloor$ will denote the greatest integer less than or equal to x. In Lemma 30, we will also have need of $\lceil x \rceil$, which denotes the least integer greater than or equal to x.

As mentioned above, in studying the plus closure, we may restrict our attention to local domains. In what follows p will denote the characteristic of the residue field of any local ring under consideration as well as the ring element $p \cdot 1$.

If $z \in (x, y)R^+$, say $z = yv + xw$ for some elements $v, w \in R^+$, then the minimal polynomial which w satisfies over R determines the minimal polynomial for v. More precisely, we have the following lemma from [1].

Lemma 3. *Let $x, y, z \in R$ with $y \neq 0$. Let $f(T) = \sum_{i=0}^{n} a_i T^{n-i}$ be a monic polynomial over R and suppose $f(w) = 0$. For each $0 \leqslant i \leqslant n$, set $b_i = (-1)^i \sum_{j=0}^{i} \binom{n-j}{i-j} a_j x^j z^{i-j}$ and let $g(T) = \sum_{i=0}^{n} b_i T^{n-i}$. Then $g(z - xw) = 0$. In addition, if each $b_i \in y^i R$, then $(z - xw)/y \in R^+$.*

Let I be an ideal of R. Recall that $z \in R$ is defined to be in the *integral closure of I*, denoted $\overline{I}$, if there exists a monic polynomial $f(T) = T^n + a_1 T^{n-1} + \cdots + a_n$ such that $f(z) = 0$ and each $a_i \in I^i$. Note that $z \in \overline{I}$ if and only if $z^n \in I(I, z)^{n-1}$ for some n.

In Section 3 we will make use of the extended Rees ring of R with respect to an ideal I. This is defined as the ring $R[It, u]$ where t is an indeterminate and $u = t^{-1}$. The ring $R[It, u]$ has a natural $\mathbb{Z}$-grading: let R be the homogeneous summand of degree zero and assign $\deg(t) = 1$. Let S denote the integral closure of $R[It, u]$. Then S is also a $\mathbb{Z}$-graded ring and for $n > 0$ the degree n summand is $\overline{I^n} t^n$. An important consequence is that the intersection of the ideal $(u^n)S$ with the degree zero summand is equal to the integral closure of I^n in R. Hence, the extended Rees ring provides a way to reduce problems about finitely generated ideals to problems about principal ideals.

When dealing with integral extensions of graded rings, we will restrict our attention to those extensions which respect the grading in the sense of the next definition.

Definition 4. An integral extension S of R is called a g-integral extension if R is a graded subring of S.

Since any ring can be given the trivial grading, any integral extension of non-graded rings can be thought of as a g-integral extension.

In Section 3 we will need some facts about the discriminant of a polynomial.

Definition 5. Let $f(T) = (T - \sigma_1) \cdots (T - \sigma_n)$. Then the discriminant of f is defined to be $\Delta_f = \prod_{i<j} (\sigma_i - \sigma_j)^2$.

It is easy to see that the discriminant is a symmetric polynomial and homogeneous of degree $2\binom{n}{2} = n(n-1)$ in $\sigma_1, \ldots, \sigma_n$. For a monomial $X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ in the variables $X_1, \ldots, X_n$, define the weight of the monomial to be $\alpha_1 + 2\alpha_2 + \cdots + n\alpha_n$. Let $a_1, \ldots, a_n$ be the elementary symmetric polynomials of $\sigma_1, \ldots, \sigma_n$. So, for example, $a_1 = \sigma_1 + \cdots + \sigma_n$ and $a_n = \sigma_1 \cdots \sigma_n$.

Theorem 6. *Let $f(\sigma) \in R[\sigma_1, \ldots, \sigma_n]$ be symmetric and homogeneous of degree d. Then there exists a polynomial $g(X_1, \ldots, X_n)$, every term of which has weight d, such that $f(\sigma) = g(a_1, \ldots, a_n)$.*

Proof. This is a simple variation of [4, Theorem 6.1, p. 191]. □

Hence, if $f(T) = T^n + a_1T^{n-1} + \cdots + a_n$, then Δ_f can be expressed as a polynomial in $a_1, \ldots, a_n$. In fact, we have the following.

Proposition 7. *Let $f(T) = T^n + a_1T^{n-1} + \cdots + a_n$. Then as a function of $a_1, \ldots, a_n$, the discriminant $\Delta_f = N(a_{n-1})^n +$ lower degree terms in a_{n-1}, where N is an integer which is a unit if $p \nmid (n-1)$.*

Proof. Since the degree of Δ_f is $n(n-1)$, by Theorem 6 we may write $\Delta_f = g(a_1, \ldots, a_n)$ for some polynomial g, every term of which has weight $n(n-1)$. Hence, as a function of a_n,

$$\Delta_f = N_0(a_{n-1})^n + N_1(a_{n-1})^{n-1} + \cdots + N_n,$$

where $N_1, \ldots, N_n$ are non-constant functions of $a_1, \ldots, a_{n-2}, a_n$ and N_0 is a constant.

Now, $g(0, \ldots, 0, -1, 0) = \pm N_0 =$ the discriminant of $f(T) = T^n - T$. It is easily seen that this discriminant equals the discriminant of $T^{n-1} - 1$. Now, it follows from the definition that this discriminant is contained in some prime ideal P if and only if $\sigma_i - \sigma_j \in P$ for two roots σ_i, σ_j of $T^{n-1} - 1$. This happens if and only if $T^{n-1} - 1$ and its derivative have a common root modulo P. Clearly, this occurs precisely when $n-1$ is in P. Hence, N_0 is a unit if $p \nmid (n-1)$. □

The next theorem is well-known. A good reference is [5, vol. 1, V, Sections 10, 11 and vol. 2, VI, Sections 11, 12].

Theorem 8. *Let $f(T) \subseteq R[T]$ be an irreducible monic polynomial of degree n and let S be the extension of R obtained by adjoining a root of f. If a height one prime qR ramifies under this extension, then q divides the discriminant of f.*

Let R be a regular local ring and $P = (x, y)R$ a height two prime ideal. We may construct a valuation on the quotient field of R as follows. Let a and b be positive integers. Let $S = R_P[t]$, where $t^a = x$. This is a two-dimensional regular local ring with maximal ideal $(t, y)S$. Now adjoin $u = y/t^b$ and consider $A = S[u]_{(t)}$. Since the maximal ideal of A is principal, A is a discrete valuation ring and there exists a valuation v on the quotient field of A defined by $v(\alpha t^n) = n$ if α is a unit of A. This restricts to a valuation on the quotient field of R. Notice that $v(x) = v(t^a) = a$ and, since u is a unit of A, $v(y) = v(ut^b) = b$. Further, we may express any element of R as a polynomial

$$f(x, y) = \sum_{(e,f)\in B} r_{(e,f)}x^e y^f$$

where each $r_{(e,f)} \notin P$ and

$$B = \left\{(e_i, f_i) \;\middle|\; 1 \leqslant i \leqslant k,\ e_1 < \cdots < e_k,\ f_1 > \cdots > f_k\right\}.$$

We claim that $v(f)$ is simply the infimum over the values of the monomials. It suffices to prove that monomials of the same value cannot sum to an element of higher value. Suppose that $v(z_1) = v(z_2) = \cdots = v(z_k)$ where $z_i = r_i x^{e_i} y^{f_i} = r_i u^{f_i} t^{ae_i+bf_i}$, $f_1 > \cdots > f_k$. Then $ae_i + bf_i = ae_j + bf_j$ for all $1 \leqslant i, j \leqslant k$. If $v(z_1 + \cdots + z_k) > ae_i + bf_i$ then $r_1 u^{f_1-f_k} + \cdots + r_{k-1} u^{f_{k-1}-f_k} + r_k = 0$ in the residue field of A. But the residue field of A is clearly $K(u)$ where K is the quotient field of R/P, so we must have $v(z_1 + \cdots + z_k) = ae_i + bf_i$.

3. Sufficient conditions

In this section we will present some conditions which ensure that an element $z \in R^+$ is actually in IR^+. The first theorem [2, Theorem 2.13] in equicharacteristic p gives the plus closure form of the generalized Briançon–Skoda theorem of Hochster and Huneke [3, p. 45].

Theorem 9. *Let R be an integral domain and $I = (x_1, \ldots, x_n)$ an ideal of R. Suppose $p \in \sqrt{(x_1, x_2)R}$ and $z \in \overline{I^{n+k}}$ with $k \geqslant 0$. Then there exists an integral extension S of R with $z \in I^{k+1}S$.*

Lemma 10. *Let R be a local ring and p the characteristic of its residue field. Then given $0 \leqslant j \leqslant i \leqslant p^n$ and an integer m relatively prime to p, there is a unit u_{ij} such that $\binom{p^n m-j}{i-j} = u_{ij}\binom{p^n-j}{i-j}$. In fact,*

$$u_{ij} = \frac{(p^n m - j)!(p^n - i)!}{(p^n m - i)!(p^n - j)!}.$$

Proof. Fix i and p as above. Write u_j for u_{ij}. Clearly, $u_i = 1$. Assume that for some $j + 1 \leqslant i$ we have such a unit u_{j+1}. Then,

$$\begin{aligned}\binom{p^n m - j}{i - j} &= \frac{p^n m - j}{i - j}\binom{p^n m - (j+1)}{i - (j+1)} = u_{j+1}\frac{p^n m - j}{i - j}\binom{p^n - (j+1)}{i - (j+1)} \\ &= u_{j+1}\frac{p^n m - j}{p^n - j}\binom{p^n - j}{i - j}.\end{aligned}$$

Thus,

$$u_j = u_{j+1}\frac{p^n m - j}{p^n - j}$$

is the desired unit. One can easily check that

$$u_{ij} = \frac{(p^n m - j)!(p^n - i)!}{(p^n m - i)!(p^n - j)!}. \qquad \square$$

Proposition 11, interesting in its own right, will be used in proving Lemma 12 below.

Proposition 11. *Let R be an integrally closed ring and let $x, y \in R$. Suppose that $z \in (x, y)R^+$ with $z = \alpha x + \beta y$ where α satisfies an irreducible monic polynomial of degree $p^n m$ over R with $(p, m) = 1$. Then $z = \alpha' x + \beta' y$, for some $\alpha', \beta' \in R^+$ where α' satisfies a polynomial of degree p^n over R.*

Proof. Let β satisfy the irreducible polynomial $f(T) = T^N + b_1 T^{N-1} + \cdots + b_N$ over R. Since $z - \beta y = \alpha x$, we must have $N = p^n m$. Since R is integrally closed, $f(T)$ is irreducible over the quotient field of R. Thus, for any root $\hat{\beta}$ of $f(T)$, there is an automorphism of R^+ taking β to $\hat{\beta}$. Hence $z - \hat{\beta} y \in xR^+$ for all roots $\hat{\beta}$ of $f(T)$. Let $g(T) = \sum_{i=0}^{N} c_i T^{N-i}$ where

$$c_i = (-1)^i \sum_{j=0}^{i} \binom{p^n m - j}{i - j} b_j y^j z^{i-j}.$$

Then by Lemma 3 the roots of $g(T)$ are $\{z - \hat{\beta} y \mid \hat{\beta} \text{ is a root of } f(T)\}$. This implies that

$$\sum_{j=0}^{i} \binom{p^n m - j}{i - j} b_j y^j z^{i-j} \in (x^i)$$

for each $0 \leqslant i \leqslant p^n m$. By Lemma 3 we need to show that there exist elements $\{c_j\}$ in R such that for $0 \leqslant i \leqslant p^n$,

$$\sum_{j=0}^{i} \binom{p^n - j}{i - j} c_j y^j z^{i-j} \in (x^i), \tag{1}$$

and such that $c_0 = 1$. By Lemma 10, we may satisfy the ith equation by taking $c_j = u_{ij} b_j$, for $0 \leqslant j \leqslant i$. But $c_j = (u_{ij}/u_{i0}) b_j$ for $0 \leqslant j \leqslant i$ also solves the ith equation and

$$\frac{u_{ij}}{u_{i0}} b_j = \frac{(p^n m - j)!(p^n)!}{(p^n m)!(p^n - j)!} b_j$$

does not depend on i, giving us a set $\{c_0, c_1, \ldots, c_{p^n}\}$ which solves all of the equations in (1) with $c_0 = 1$, as desired. □

Lemma 12. *Let R be integrally closed and let x, y be nonunit elements of R. Let $q_1 R, q_2 R, \ldots, q_k R$ be height one primes of R such that $x, y \notin q_i R$ for all i. Let w be an element of R^+ with $w = \alpha x + \beta y$ for some α, β integral over R. Then there exist α', β' integral over R such that $w = \alpha' x + \beta' y$ and none of $q_1 R, \ldots, q_k R$ ramify under the extension to $R[\alpha']$. If in addition $\alpha \in x^d \overline{R[\alpha]}$ for $d \leqslant 1$, then we can ensure that $\alpha' \in x^d \overline{R[\alpha']}$.*

Proof. Let $f(T) = T^n + a_1T^{n-1} + \cdots + a_n$ be the monic irreducible polynomial over R which has α as a root. We may assume that p does not divide $n-1$, for otherwise p and n are relatively prime and by Lemma 11 we may take $\alpha' \in R$. If β satisfies $T^n + b_1T^{n-1} + \cdots + b_n$ over R, then

$$b_i y^i = (-1)^i \sum_{j=0}^{i} \binom{n-j}{i-j} a_j x^j w^{i-j}.$$

Let $a'_i = a_i$ for $i \neq n-1$ and $a'_{n-1} = a_{n-1} + lx^{n-1}y^n$, where $l \in R$ will be chosen later in the proof. Let $b'_i = b_i$ for $i < n-1$, $b'_{n-1} = b_{n-1} + (-1)^{n-1}lx^{2(n-1)}y$, and $b'_n = b_n + (-1)^n lx^{2(n-1)}w$. Then for $i < n-1$ certainly

$$(-1)^i \sum_{j=0}^{i} \binom{n-j}{i-j} a'_j x^j w^{i-j} = b'_i y^i.$$

When $i = n-1$, this same sum is

$$(-1)^{n-1} \sum_{j=0}^{n-1} \binom{n-j}{n-1-j} a'_j x^j w^{n-1-j} = b_{n-1}y^{n-1} + (-1)^{n-1}lx^{2(n-1)}y^n = b'_{n-1}y^{n-1}.$$

Similarly, when $i = n$,

$$(-1)^n \sum_{j=0}^{n} \binom{n-j}{n-j} a'_j x^j w^{n-j} = b_n y^n + (-1)^n lx^{2(n-1)}y^n w = b'_n y^n.$$

Let α' be a root of $\sum_{i=0}^{n} a'_i T^{n-i}$. Then by Lemma 3, $\beta' = (w - \alpha' x)/y$ is a root of $\sum_{i=0}^{n} b'_i T^{n-i}$. Hence $w = \alpha' x + \beta' y$. Also, since $\alpha \in x^d \overline{R[\alpha]}$, it follows that $a_i \in x^{di} R$ for all i. Then for $d \leqslant 1$, $a'_i \in x^{di} R$ for all i as well. Hence $\alpha' \in x^d \overline{R[\alpha']}$.

Finally, we show that we may choose l such that $q_1R, \ldots, q_kR$ do not ramify. By Theorem 8, it suffices to prove that there exists an l such that for each i, q_i does not divide the discriminant of $\sum_{j=0}^{n} a'_j T^{n-j}$. Denote this discriminant by $\Delta(l)$. Since we are assuming that p does not divide $n-1$, by Proposition 7 for some unit integer N,

$$\begin{aligned}\Delta(l) &= N\left(a_{n-1} + lx^{n-1}y^n\right)^n + \text{lower degree terms in } a_{n-1} + lx^{n-1}y^n \\ &= \left(Nx^{n(n-1)}y^{n^2}\right)l^n + \text{lower degree terms in } l.\end{aligned}$$

Modulo q_i, the coefficient $Nx^{n(n-1)}y^{n^2} \not\equiv 0$ and so considering l to be an indeterminate, $\Delta(l) \not\equiv 0$. Modulo q_i there are at most n congruence classes which give roots of $\Delta(l)$.

Without loss of generality, we may assume that $q_1 = p$. Let $A = \{ky^j \mid 1 \leqslant k < p, j \geqslant 1\}$. This is an infinite set, all of whose members are distinct modulo p. So there exists some $ky^j \in A$ such that $\Delta(ky^j) \not\equiv 0$ modulo p.

Now we consider q_i for $i \geqslant 2$. The set $B = \{my^j \mid m \geqslant 1\}$ is an infinite set, all of whose members are distinct modulo q_i. Thus, for each $i \geqslant 2$, there exists an integer m_i such that if $m \geqslant m_i$ then $\Delta(my^j) \not\equiv 0$ modulo q_i. Let $M = \max\{m_2, \ldots, m_k\}$ and let $l = (Mp+k)y^j$. Then certainly $\Delta(l) \not\equiv 0$ modulo q_i for $i \geqslant 2$ and since $l \equiv ky^j$ modulo p, $\Delta(l) \not\equiv 0$ modulo p. □

The information about the coefficients of the polynomial in the next proposition will be useful in Section 4.

Proposition 13. *Let x, y be nonunit elements of an integrally closed ring R, let p be an odd prime number, and let $n = p^2$. Suppose that $p \in (y^c, x^{de})R$ where c, d, e, f are rational numbers such that $1/c + 1/d \leqslant f/3$ and $1/3 \leqslant e \leqslant 1$. Also suppose $z \in R^+$ satisfies $z^3 \in (y^c, x^d)^f R$. Further assume there exists $F \in R$ such that $z^{n-1} - Fx^{n-1}y^{n-1} \in (y^n, x^n)R$. Then there exist elements v, w integral over R such that $z = yv + xw$ where w can be chosen to be any root of $T^n + a_1T^{n-1} + \cdots + a_n = 0$, with each a_i in an integral extension S of R. We may choose our coefficients so that, modulo the integral closure of some fractional power of x in S, $a_i \equiv 0$ for $i < n-1$, $a_{n-1} \equiv -Fy^{n-1}$, and $a_n \equiv r$ for some element $r \in R$. Furthermore, we can ensure that if qR is a height one prime with $x, y \notin qR$ and $z^3 \in qR$, then qR does not ramify under the extension to $S[w]$.*

Proof. Suppose that $c = c_1/c_2$ and $d = d_1/d_2$ where c_1, c_2, d_1, d_2 are integers. Let $R' = R[z, s, u]$, where $s^{3c_2} = y$ and $u^{3d_2} = x$. We shall construct the polynomial $T^n + a_1T^{n-1} + \cdots + a_n$ and let w be a root. By Lemma 3 with $a_0 = 1$, we will have v integral over R if for some integral extension S of R we satisfy

$$\sum_{j=0}^{i} \binom{n-j}{i-j} a_j u^{3d_2 j} z^{i-j} = b_i s^{3c_2 i}$$

with $b_i \in S$ for $i = 1, \ldots, n$. We inductively define $a_1, \ldots, a_{n-1}$ to satisfy the first $n-1$ equations and also to satisfy

$$a_j u^{3d_2 j} \in \left(s^{3c_1}, u^{3d_1 e}\right)\left(s^{c_1}, u^{d_1}\right)^{fj-1}\overline{\left(s^{c_1}, u^{d_1}\right)S_j},$$

where S_j is an integral extension of R' and $S_j \subseteq S_i$ for $j < i$. We then let $S = S_n$. To satisfy the ith equation, we must define a_i, b_i so that

$$\sum_{j=0}^{i-1} \binom{n-j}{i-j} a_j u^{3d_2 j} z^{i-j} = b_i s^{3c_2 i} - a_i u^{3d_2 i}.$$

Of course, $a_0 = 1$.

First consider $i < n$. Since $z^3 \in (s^{c_1}, u^{d_1})^{3f} R'$, it follows that $z^i \in \overline{(s^{c_1}, u^{d_1})^{fi} R'}$. Hence,

$$a_j u^{3d_2 j} z^{i-j} \in \left(s^{3c_1}, u^{3d_1 e}\right)\left(s^{c_1}, u^{d_1}\right)^{fj-1}\overline{\left(s^{c_1}, u^{d_1}\right)^{f(i-j)+1} S_j} \quad \text{for } j \neq 0.$$

Applying Theorem 9 we see that

$$\overline{\left(s^{c_1}, u^{d_1}\right)^{fi-fj+1} S_j} \subseteq \left(s^{c_1}, u^{d_1}\right)^{fi-fj} S_{j_0}$$

for some integral extension S_{j_0} of S_j. When $j = 0$ and $i < n$, the term

$$\binom{n}{i} z^i \in p\overline{\left(s^{c_1}, u^{d_1}\right)^{fi} R'} \subseteq \left(s^{3c_1}, u^{3d_1 e}\right)\left(s^{c_1}, u^{d_1}\right)^{fi-1}\overline{\left(s^{c_1}, u^{d_1}\right) S_{i_1}},$$

where S_{i_1} is an integral extension of R'. Let S_i be an integral extension of R' containing S_{i_0} and S_{j_0} for $1 \leqslant j < i$. Then the left-hand side of the equation is in $(s^{3c_1}, u^{3d_1 e})(s^{c_1}, u^{d_1})^{fi-1}\overline{(s^{c_1}, u^{d_1})S_i}$. Any generator of $(s^{3c_1}, u^{3d_1 e})(s^{c_1}, u^{d_1})^{fi-1}$ which is not a multiple of $s^{3c_2 i}$ must be a multiple of u^l, where $l \geqslant d_1(fi - 1 - 3(c_2/c_1)i + 1/c_1) + 3d_1 e$. Since $c_2/c_1 \leqslant f/3 - d_2/d_1$, we obtain

$$l \geqslant 3d_2 i - d_1 + d_1/c_1 + 3d_1 e > 3d_2 i, \quad \text{since } 3e \geqslant 1.$$

So we may solve the equation with $a_i u^{3c_2 i} \in (s^{3c_1}, u^{3d_1 e})(s^{c_1}, u^{d_1})^{fi-1}\overline{(s^{c_1}, u^{d_1})S_i}$. Notice that since $l > 3d_2 i$, we may choose $a_i \in uS_i$, which implies that $a_i \in u\overline{R'[a_i]}$.

Let $q_1, \ldots, q_k$ be the height one primes with the property that $z^3 \in q_i R$ and $x, y \notin q_i R$. Before proving the final statement of the proposition, we will first show that for these primes there is no ramification under the extension to $R[a_1, \ldots, a_n]$. To this end, suppose that we have chosen $a_1, \ldots, a_{i-1}$ such that $q_1 R, \ldots, q_k R$ do not ramify under the extension to $R'[a_1, \ldots, a_{i-1}]$. Let

$$w_i = \sum_{j=0}^{i-1} \binom{n-j}{i-j} a_j u^{3d_2 j} z^{i-j}.$$

Then $w_i = b_i s^{3c_2 i} - a_i u^{3d_2 i}$. By Lemma 12 we may replace our original choice of a_i, b_i with elements a_i', b_i', integral over R with the additional property that $q_1 R, \ldots, q_k R$ do not ramify under the extension to $R'[a_i']$. Note that Lemma 12 allows us to maintain our assumption that $a_i \in u\overline{R'[a_i]}$.

Finally, the $i = n$ case differs only in the $j = 0$ term. Thus the left-hand side of the equation equals $z^n + G$ where

$$G \in \left(s^{3c_1}, u^{3d_1 e}\right)\left(s^{c_1}, u^{d_1}\right)^{fn-1}\overline{\left(s^{c_1}, u^{d_1}\right) S_n} \subseteq \left(u^{3d_2 n}, s^{3c_2 n}\right) S_n.$$

Say $G = u^{3d_2 n}\alpha + s^{3c_2 n}\beta$, where we have chosen α as above so that $\alpha \in \overline{uR'[\alpha]}$ and $q_1 R, \ldots, q_k R$ do not ramify under the extension to $R'[\alpha]$. Now,

$$z^n - Fs^{3c_2(n-1)} u^{3d_2(n-1)} z = u^{3d_2 n} r_1 + s^{3c_2 n} r_2$$

for some elements $r_1, r_2 \in R$. Replacing a_{n-1} with $a_{n-1} - Fu^{3d_2(n-1)}$ still allows us to solve the $(n-1)$st equation (with a different b_{n-1}) and also enables us to solve the nth equation since the left-hand side of that equation is now

$$z^n + G - Fs^{3c_2(n-1)}u^{3d_2(n-1)}z = u^{3d_2n}(r_1 + \alpha) + s^{3c_2n}(r_2 + \beta).$$

In fact, we may choose $a_n = r_1 + \alpha$, satisfying the desired condition.

To prove the final statement, we may now apply Lemma 12 to the equation $z = yv + xw$ to show that $q_1R, \ldots, q_kR$ do not ramify under the extension to $S[w]$. Recall that in the proof of Lemma 12 no changes are made to $a_1, \ldots, a_{n-2}$ and a_n, while a_{n-1} is replaced by $a_{n-1} + ly^{n-1}x^n$. So the coefficients of the new polynomial will also satisfy the desired conditions. □

Theorem 16 below and its corollaries are our strongest sufficient conditions. The first lemma is [1, Lemma 2.5]. The statement here is slightly stronger, but this is what is actually proven in [1].

Lemma 14. *Suppose i, j are positive integers and $n = i + j$. Let $a_k \ldots a_0$ be the expression for i in base p, i.e., $i = a_0 + a_1p + \cdots + a_kp^k$ with $0 \leqslant a_j < p$. Similarly, suppose $j = b_k \ldots b_0$, $n = c_k \ldots c_0$. Let $d = |\{j \mid a_j + b_j > c_j\}|$. Then d is the highest power of p which divides $\binom{n}{i}$.*

Lemma 15. *Let $I = (s, u)$ be an ideal of R and q, e, f, h be positive integers with $e + f > q \geqslant f + 2$ and $q \geqslant e$. Further assume $s^j \in (u^{\lfloor (e+f-q)j/e \rfloor})R$ for every j. Then*

(i) $I^{qj} \subseteq (s^{ej}, u^{fj})$ *and*
(ii) $I^{hq(q-1)} \subseteq [s^{ehq}, u^{fhq}, (s^eu^{q-e})I^{hq(q-1)-q}]$.

Proof. This is routine and is left to the reader. □

Theorem 16. *Let R be a $\mathbb{Z}$-graded integral domain. Let $\mu \in R$ such that $\mu^p = p$. Let s, u, z be homogeneous elements of R with* $\deg(s) = \deg(z) = 0$, $\deg(u) = -1$. *Let $I = (s, u)\overline{R}$. Suppose e, f, q are positive integers with $e + f > q \geqslant f + 2$. Further assume $z \in \overline{I^q}$, $\mu z^j \in I^{qj}$, and $s^j \in (u^{\lfloor (e+f-q)j/e \rfloor})$. Then there exists a g-integral extension S of R and elements $\alpha, \beta \in S$ such that $z = s^e\alpha + u^f\beta$, where α is homogeneous of degree zero.*

Proof. As in the proof of [1, Theorem 2.8], we may reduce to the Noetherian case by replacing R with a Noetherian subdomain in which the entire hypothesis is satisfied. (In our case, we must also note that the condition that $s^j \in (u^{\lfloor (e+f-q)j/e \rfloor})$ for every j is equivalent to the condition that $s^j \in (u^{\lfloor (e+f-q)j/e \rfloor})$ for every $j \leqslant e$. This only requires the existence of a finite set of elements satisfying a finite set of equations.)

Next we derive an equation for z^n, for some large n, which will be used in the final step of the proof. To this end, define a family of modules

$$C_i = \left(I^q, z\right)^i \Big/ \left(s^{ei}, u^{fi}\right)$$

and homomorphisms $g_{ij}: C_i \to C_j$ with $i < j$ by $g_{ij}(\bar{c}) = \overline{(s^e u^{q-e})^{j-i} c}$. This map is well-defined since $s^e \in (u^{e+f-q})R$. Now, as $z \in \overline{I^q}$, there exists a positive integer h such that $z^{h+1} \in I^q(I^q, z)^h$. We claim that for every $N \geqslant hq$, $I^{q(N-h)} \subseteq (s^{eN}, u^{fN}, (s^e u^{q-e}) I^{q(N-h)-q})$. This is true for $N = hq$ by Lemma 15(ii). Assume that this holds for some $N \geqslant hq$ and consider $I^{q(N+1-h)} = I^{q(N-h)} I^q$. Since Lemma 15(i) gives $I^q \subseteq (s^e, u^f)$, it follows that

$$I^{q(N+1-h)} \subseteq \left(s^{e(N+1)}, u^{f(N+1)}, \left(s^e u^{q-e}\right) I^{q(N+1-h)-q}\right),$$

which proves the claim. Using the integer h mentioned above, the condition $z^{h+1} \in I^q(I^q, z)^h$ implies that $(I^q, z)^N = I^{q(N-h)}(I^q, z)^h$ for all $N > h$. This implies that every nonzero monomial in C_N, $N \geqslant hq$, will be divisible by $s^e u^{q-e}$ and so $C_N = g_{N-1,N}(C_{N-1})$. Hence, $g_{N-1,N}$ is onto for every $N \geqslant hq$. Thus, $C = \varinjlim C_i$ is a homomorphic image of C_{hq-1} and so it is a Noetherian module. We then see that $\bigcup \ker(g_{hq-1,j})$ is finitely generated and it follows that $C = C_M$ for sufficiently large M.

Now, to obtain the desired equation, for each positive integer k, since z^{p^k} is an element of C_{p^k}, it is an element of C. Let $B = \{\overline{z^{p^k}} \mid k \geqslant 1\}R$. Since B is a submodule of C, it is finitely generated and so there exists an integer K with $B = \{z^{p^k} \mid 1 \leqslant k \leqslant K\}R$. Choose L sufficiently large so that $p^L > \max\{M, p^K\}$. Then, as $\overline{z^{p^L}} \in B$, we obtain an equation

$$z^{p^L} = \sum_{k=1}^{K} r_k \left(s^e u^{q-e}\right)^{p^L - p^k} z^{p^k} + s^{ep^L} v + u^{fp^L} w \tag{2}$$

with $\deg(r_k) = (q-e)(p^L - p^k)$, $\deg(v) = 0$, and $\deg(w) = fp^L$. We will apply this equation later in the proof.

Let $n = p^L$. By Lemma 3, to obtain $z - s^e \alpha = u^f \beta$ it suffices to find elements $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ such that

$$\sum_{j=0}^{i} \binom{n-j}{i-j} a_j s^{ej} z^{i-j} = u^{fi} b_i,$$

for $1 \leqslant i \leqslant n$, where $\deg(a_j) = 0$. We will define the elements $a_1, \ldots, a_n$ indirectly by choosing elements $c_1, \ldots, c_n$ such that $a_n = c_n - v$, $a_i = c_i - r_k u^{(q-e)(p^L - p^k)}$, for $i = p^L - p^k$ and $1 \leqslant k \leqslant K$, and $a_i = c_i$ otherwise. We will require that $c_i \in \mu^{\phi(i)} I^{(q-e)i}$ for each i, where $\phi(i)$ denotes the sum of the digits when $p^L - i$ is written in base p. To obtain $\deg(a_i) = 0$ it suffices to ensure that $\deg(c_i) = 0$ for all i. Simultaneously, recalling that $s^e \in (u^{e+f-q})R$, we will choose $d_1, \ldots, d_n$ and set $b_n = d_n + w$, $b_i = d_i - r_k(s^e/(u^{e+f-q}))^{p^L - p^k}$, for $i = p^L - p^k$, $1 \leqslant k \leqslant K$, and $b_i = d_i$ otherwise.

We choose c_1 as follows. The first equation is $\binom{p^L}{1} z + \binom{p^L - 1}{0} a_1 s^e = u^f b_1$. As $c_1 = a_1$ and $d_1 = b_1$, this can be written as $p^L z + c_1 s^e = u^f d_1$, or alternatively, since $\mu^p = p$, as $\mu^{pL} z + c_1 s^e = u^f d_1$. Now by Lemma 15, $\mu z \in I^q \subseteq (s^e, u^f)$ and has degree 0. So we may solve this equation with $c_1 \in \mu^{pL-1} I^{q-e}$ and $\deg(c_1) = 0$. Now, $\phi(1) = (p-1)L$ as $p^L - 1$ has L digits, each equalling $(p-1)$. As $(p-1)L \leqslant pL - 1$, we have in fact chosen $c_1 \in \mu^{\phi(1)} I^{q-e}$.

Suppose that for each $j < i$ we have chosen $c_j \in \mu^{\phi(j)} I^{(q-e)j}$ with $\deg(c_j) = 0$ so that the first $i-1$ equations are satisfied. We need to find c_i, d_i satisfying

$$\sum_{j=0}^{i-1} \binom{n-j}{i-j} a_j s^{ej} z^{i-j} + a_i s^{ei} = u^{fi} b_i.$$

If $i < p^L$ one can easily check that $u^{fi} b_i - s^{ei} a_i = u^{fi} d_i - s^{ei} c_i$. Let E be the smallest integer such that $p^L - p^E < i$. Then the equation we must satisfy becomes

$$\binom{p^L}{i} z^i + \sum_{j=1}^{i-1} \binom{n-j}{i-j} c_j s^{ej} z^{i-j} - \sum_{k=E}^{K} \binom{p^k}{i+p^k-p^L} r_k \left(s^e u^{q-e}\right)^{(p^L-p^k)} z^{i+p^k-p^L} = u^{fi} d_i - s^{ei} c_i.$$

(The final sum is vacuous if $E > K$.) To find $c_i \in \mu^{\phi(i)} I^{(q-e)i}$, by Lemma 15 it suffices to show each term is in $\mu^{\phi(i)} I^{qi}$. Since each term in the left-hand side of the equation has degree zero, we may then choose c_i to be homogeneous of degree zero.

By [1, Theorem 2.8], $\mu^{\phi(i)+1} \mid \binom{p^L}{i}$. As $\mu z^i \in I^{qi}$, this yields $\binom{p^L}{i} z^i \in \mu^{\phi(i)} I^{qi}$. Similarly, this same result gives

$$\binom{n-j}{i-j} c_j s^{ej} z^{i-j} \in \mu^{\phi(i)-\phi(j)+1} \mu^{\phi(j)} I^{qj} z^{i-j} \subseteq \mu^{\phi(i)} \left(\mu z^{i-j}\right) I^{qj} \subseteq \mu^{\phi(i)} I^{qi}.$$

The last term is

$$\binom{p^k}{i+p^k-p^L} r_k \left(s^e u^{q-e}\right)^{(p^L-p^k)} z^{i+p^k-p^L} \in \mu^{\phi(i)+1} I^{q(p^L-p^k)} z^{i+p^k-p^L} \subseteq \mu^{\phi(i)} I^{qi}.$$

Therefore, we may find the appropriate c_i for $i < n = p^L$.

Finally, let $i = p^L$. Since the binomial coefficient is $\binom{n-j}{n-j} = 1$, the equation we must solve is

$$\sum_{j=0}^{n-1} a_j s^{ej} z^{n-j} + a_n s^{en} = u^{fn} b_n.$$

Substituting c_j's and d_j's this becomes

$$z^n + \sum_{j=1}^{n-1} c_j s^{ej} z^{n-j} - \sum_{k=1}^{K} r_k \left(s^e u^{q-e}\right)^{p^L-p^k} z^{p^k} + c_n s^{en} - v s^{en} = u^{fn} d_n + u^{fn} w.$$

After applying Eq. (2) with $p^L = n$, this simplifies to

$$\sum_{j=1}^{n-1} c_j s^{ej} z^{n-j} = u^{fn} d_n - c_n s^{en}.$$

Now $c_j s^{ej} \in \mu^{\phi(j)} I^{qj} \subseteq \mu I^{qj}$ for all j and since $\mu z^{n-j} \in I^{q(n-j)}$, each term in the left-hand sum is contained in I^{qn}. As usual, this allows us to find the desired c_n, d_n to complete the proof. (Again, since each term of the summation has degree 0, we can ensure that $\deg(c_n) = 0$.) □

Corollary 17. *Let R be an integrally closed integral domain and $I = (x_1, \ldots, x_{k+1})$ an ideal with $p \in \sqrt{I}$. Suppose $a, b_1, \ldots, b_k, c, d$ are positive integers such that $c > b_1$ and $t_1, \ldots, t_k \in I$ with $z^a \in \overline{(t_1^{b_1}, \ldots, t_k^{b_k}, I^c)^d}$ where $1/b_1 + \cdots + 1/b_k + k/c \leqslant d/a$. Then $z \in IR^+$.*

Proof. Replace R by $R[\mu]$ where $\mu^p = p$. Since $p \in \sqrt{I}$, there exists an integer m such that $\mu^m \in I^{2k}$. Let $g = b_1 \cdots b_k m$, $e_i = b_1 \cdots b_k cm/b_i$, for $1 \leqslant i \leqslant k$, and $q = e_1 + \cdots + e_k + kg$. Let $A = R[\mu, s_1, \ldots, s_k, v_1, \ldots, v_{k+1}]$ with $s_i^{e_i} = t_i$, and $v_i^g = x_i$. Let $J = (v_1, \ldots, v_{k+1})A$. Then

$$z^a \in \overline{(s_1, \ldots, s_k, J)^{b_1 \cdots b_k cdm} A}$$

and so

$$z^j \in \overline{(s_1, \ldots, s_k, J)^{(e_1+\cdots+e_k+kg)j} A} = \overline{(s_1, \ldots, s_k, J)^{qj} A}$$

for every j. Now $\mu^m \in I^{2k} \subseteq J^{2kg} \subseteq J^{2km}$ and so $\mu \in \overline{J^{2k}}$. Thus for every j, $\mu z^j \in \overline{(s_1, \ldots, s_k, J)^{qj+2k}} A$. By Theorem 9, this implies that for every j, $\mu z^j \in (s_1, \ldots, s_k, J)^{qj} A'$ for some integral extension A' of A. Also, note that $s_i^{e_i} \in J^g$ and so $s_i^j \in \overline{J^{\lfloor gj/e_i \rfloor}}$ for all j.

Let $\widetilde{J}$ be the ideal $(s_2, \ldots, s_k, J)A'$ and let S be the integral closure of the extended Rees ring, $A'[\widetilde{J}t, u]$, where $u = t^{-1}$. This is a graded ring in which the intersection of the ideal (u^n) with the degree zero summand is equal to the integral closure of $\widetilde{J}^n$ in A'.

Note that we now have $s_1^j \in (u^{\lfloor gj/e_1 \rfloor})S$, $z^j \in \overline{(s_1, u)^{qj}}$, $\mu z^j \in (s_1, u)^{qj}$, and $s_1^j, z^j, \mu z^j$ all have degree zero. We may now apply Theorem 16 with $e = e_1$ and $f = q - e_1 + g$, replacing m if necessary by a larger integer to ensure $e_1 \geqslant g + 2$. This gives $z - s_1^{e_1}\alpha = u^{q-e_1+g}\beta$ for some α, β in a g-integral extension of R with $\deg(\alpha) = 0$. The intersection of the degree zero summand of S with $(u^{q-e_1+g})S$ is equal to

$$\overline{(s_2, \ldots, s_k, J)^{e_2+\cdots+e_k+(k+1)g}} A' \subseteq (s_2, \ldots, s_k, J)^{e_2+\cdots+e_k+(k+1)g-2k+1} R^+,$$

by Theorem 9. This last ideal is contained in $(s_2^{e_2}, \ldots, s_k^{e_k}, J^{(k+1)g-k})R^+$. Now,

$$J^{(k+1)g-k} = (v_1, \ldots, v_{k+1})^{(k+1)g-k} \subseteq \left(v_1^g, \ldots, v_{k+1}^g\right) = I.$$

Hence $(s_2^{e_2}, \ldots, s_k^{e_k}, J^{(k+1)g-k})R^+ \subseteq IR^+$, which completes the proof. □

Corollary 18. *Let R be an integrally closed integral domain and $I = (x, y)$ an ideal with $p \in \sqrt{I}$. Let a, b, c, d be positive integers with $c > b$ and $1/b + 1/c \leqslant d/a$. Suppose $z^a \in \overline{(t^b, I^c)^d}\, R$ where $t \in I$. Then $z \in IR^+$.*

Proof. This is the $k = 1$ case of Corollary 17 and will be used to prove the converse of Conjecture 2. □

We can now prove the reverse implication of Conjecture 2. Condition (3) represents the best information that Corollary 18 gives when $z^3 \in R$.

Corollary 19. *Let R be a regular local ring and let x, y be part of a regular system of parameters for R. Suppose p is a prime number and $p \in I = (x, y)R$. Let $z^3 \in R$ and suppose that one of the following holds*:

(1) $z^3 \in t^3R$ *for some* $t \in I$;
(2) $z^3 \in I^6$;
(3) $z^3 \in (t, I^3)^4$, $(t, I^2)^5$, *or* (t^5, I^8) *for some* $t \in I$.

Then $z \in IR^+$.

Proof. If $z^3 \in t^3R$, then z/t is integral over R. Hence $z \in tR^+$. If $z^3 \in I^6$, then $z \in \overline{I^2}$ and then Theorem 9 implies that $z \in IR^+$. The remaining cases follow directly from Corollary 18. □

4. Necessary conditions

The following lemma is [2, Lemma 3.2] and is a powerful tool for proving that elements are not in the plus closure.

Lemma 20. *Let R be an integrally closed Henselian domain with residue field K. Suppose $z \in R^+$ is in the integral closure of $(x, y)R$, a height two ideal. Let P be a height one prime containing x and let S be the integral closure of R/P. Let $f(T) \in R[T]$ be the monic irreducible polynomial satisfied by z. Let $\overline{f}(T) \in S[T]$ be the image of $f(T)$ and let $g(T) = y^{-n}\overline{f}(yT)$ with $n = \deg(f(T))$. Then $g(T) \in S[T]$. Further, if $z \in (x, y)R^+$ and, modulo the maximal ideal, $\overline{g}(T) \in K[T]$, then $g(T)$ is a power of a single irreducible factor.*

Lemma 21. *Let R be a local ring which is a unique factorization domain and p a prime which is the characteristic of the residue field of R. Let S be the integral closure of $R[z]$ where $z^n \in R$, n is prime, and either $p \mid z^n$ or $p \neq n$. Then if $q^n \nmid z^n$ for all nonunits $q \in R$, it follows that $S = R \oplus Rz \oplus L$ for some L.*

Proof. Let K be the quotient field of R and let $\alpha \in S$. Then $\alpha = a_0 + a_1z + \cdots + a_{n-1}z^{n-1}$ for some $a_0, \ldots, a_{n-1} \in K$. We wish to show that $a_0, a_1 \in R$. Let q be any prime element

of R and define a valuation v' of K by letting $v'(r)$ be the highest power of q dividing r for $0 \neq r \in R$. (Thus $R_{(q)}$ is the valuation ring.) Let v be an extension of v' to the quotient field of $R[z]$.

First suppose that $v'(z^n) = k$, where $1 \leqslant k < n$. Then $v(z) = k/n$. Now,

$$v(\alpha) \geqslant \min_{0 \leqslant j \leqslant n-1} \{v(a_j z^j)\} = \min_{0 \leqslant j \leqslant n-1} \{jk/n + v(a_j)\}$$

and equality holds if there is a unique minimum. If $jk/n - ik/n$ is an integer, then n must divide $(j-i)k$ which is impossible for n prime. Thus we see that a unique minimum exists and so $v(\alpha) = \min_{0 \leqslant j \leqslant n-1}\{jk/n + v(a_j)\}$. Since α is integral over $R[z]$, we know that $\alpha^n = r_1\alpha^{n-1} + \cdots + r_n$ for some $r_1, \ldots, r_n \in R$. Thus, $nv(\alpha) \geqslant \min_{1 \leqslant i \leqslant n}\{v(r_i) + (n-i)v(\alpha)\}$, so that $nv(\alpha) \geqslant v(r_i) + (n-i)v(\alpha)$, for some i. Thus, $v(\alpha) \geqslant v(r_i)/i$. Hence $v(\alpha) \geqslant 0$. Since $v(\alpha) = \min_{0 \leqslant j \leqslant n-1}\{jk/n + v(a_j)\}$, it follows that $v(a_j) \geqslant -jk/n$ for all j. Hence $v(a_0) \geqslant 0$ and $v(a_1) \geqslant -\lfloor k/n \rfloor = 0$.

Next suppose that $v'(z^n) = 0$ and hence $v(z) = 0$. Since we know $\Delta a_i \in R$ for all i where Δ denotes the discriminant of the polynomial $T^n - z^n$ (noting that $\Delta \in R$), we must have $0 \leqslant v(\Delta a_i) = v(\Delta) + v(a_i)$. The roots of $T^n - z^n$ are $\sigma_1 z, \sigma_2 z, \ldots, \sigma_n z$, where $\sigma_1, \ldots, \sigma_n$ are the roots of $T^n - 1$. Then

$$\Delta = \prod_{i,j} (\sigma_i z - \sigma_j z)^2 = \prod_{i,j} \left[z(\sigma_i - \sigma_j)\right]^2 = z^{n(n-1)} \prod_{i,j} (\sigma_i - \sigma_j)^2.$$

So if q divides Δ, we must have $q \mid \Delta_1$ where Δ_1 denotes the discriminant of $f(T) = T^n - 1$. This implies that $f(T)$ has a double root, say σ_i, over $R/(q)$. This would imply that σ_i is also a root of $f'(T) = nT^{n-1}$ modulo q and thus that $n = 0$ in $R/(q)$. But n is a prime number either different from p, and hence a unit in R, or equal to p and dividing z^n. But if $n \mid z^n$, then since $q \nmid z^n$, we cannot have $n \in (q)R$. Hence $v(\Delta) = 0$ and so $v(a_i) \geqslant 0$ for each i.

We have now shown that $a_0, a_1 \in R_{(q)}$ for all prime elements $q \in R$. Thus $a_0, a_1 \in R$, as desired. □

Lemma 22. *Let R be a local ring with maximal ideal I which is a unique factorization domain. Suppose n, p are primes with $p \in I$. Let S be the integral closure of $R[z]$ where $z^n \in R$ and either $p \neq n$ or $p \mid z^n$. Then $z \in IS \Leftrightarrow z^n \in t^n R$ for some element $t \in IR$.*

Proof. The reverse implication is obvious since $z/t \in S$. For the forward implication, note that R is a unique factorization domain and if $z^n \notin t^n R$ for any such t, then by Lemma 21, $S = R \oplus Rz \oplus L$, for some L. It quickly follows that $z \notin (x, y)S$. □

Proposition 23. *Let R be a Henselian regular local ring of dimension 2 with maximal ideal $I = (x, y)R$ and suppose $p > 3$ is prime with $p \in I$. If $z^3 \in R$ and $z \in IR^+$, then either $z^3 \in I^4$ or $z^3 \in t^3 R$ for some element $t \in (x, y)R$.*

Proof. We shall assume $z \in IR^+$, $z^3 \notin I^4$, and $z^3 \notin t^3R$ for any element $t \in (x, y)R$ and derive a contradiction. As $z^3 \in I^3$ by [2, Lemma 3.1], we may write

$$z^3 = Ax^3 + Bx^2y + Cxy^2 + Dy^3,$$

where at least one of the coefficients is a unit. Using a linear change of variable if necessary, we may assume D is a unit. If D is not a cube in R, we may replace R by $R[d]$, where $d^3 = D$ without affecting our hypotheses or assumptions. If $z \in R[d]$ then $z \in IR^+ \cap R[d] = IR[d]$ since the rings are regular local. But then $z = t(r_0 + r_1d + r_2d^2)$ which implies that $z^3 \in t^3R[d]$. Hence the irreducible polynomial satisfied by z is $f(T) = T^3 - z^3$. Applying Lemma 20, we have $g(T) = T^3 - D$ and we can conclude that $T^3 - D = (T - d)(T^2 + dT + d^2)$ is a power of a single irreducible polynomial. This is clearly false for $p \neq 3$. □

Lemma 24. *Let R be a Henselian regular local ring of dimension 2 with maximal ideal $I = (x, y)R$ which has a separably closed residue field and suppose $p > 3$ is a prime with $p \in I$. If $z^3 - vx^2y^2 \in I^5$ where v is a unit, then $z \notin IR^+$.*

Proof. We assume that $z \in IR^+$, say with $z = \alpha x + \beta y$, and obtain a contradiction. First, we claim that either $z^3 \in xR$ or $z^3 \in yR$. Let $S_0 = R[u, s]$ where $u^3 = x$ and $s^3 = y$. Then $z^3 - vs^6u^6 \in (u^3, s^3)^5S_0$, so $z^3 \in (s^2, u^2)^6S_0$. In fact, letting $n = p^2$, we have

$$z^{n-1} - F\big(s^2\big)^{n-1}\big(u^2\big)^{n-1} \in \big(s^{2n}, u^{2n}\big)S_0,$$

where $F = v^{(n-1)/3}$ is a unit. Thus we may apply Proposition 13, with $c = d = e = 1$ and $f = 6$. We then obtain elements $a, b \in R^+$ such that $z = s^2a + u^2b$ and b satisfies $f(T) = T^n + a_1T^{n-1} + \cdots + a_n$ over S_1, an integral extension of S_0. In addition, modulo the integral closure of a fractional power of u, $a_i \equiv 0$ for $i < n - 1$, $a_{n-1} \equiv -Fs^{2(n-1)}$, and $a_n \equiv r$, for some $r \in S_0$. Since z is also equal to $\alpha s^3 + \beta u^3$ it is easily seen that this implies that $b \in (s^2, u)R^+$. We will apply Lemma 20 to the element b with u in place of x and s^2 in place of y.

Let S denote the integral closure of $S_1[z]$. Suppose that $f(T)$ is irreducible over S. Let P be a height one prime of S containing u. Working modulo P, we have

$$\overline{f}(T) = T^n - \overline{Fs^{2(n-1)}}T + \overline{r}.$$

By Lemma 20, the element $\alpha = \overline{r/s^{2n}}$ is integral over S/P. Hence, α is in the integral closure of S_0/uS_0. Now S_0/uS_0 is isomorphic to a degree three extension of R/xR. Since no inseparability is possible in a degree three extension, the integral closure of S_0/uS_0 has the same residue field as R since that residue field is separably closed. As in Lemma 20, we let $g(T) = s^{-2n}\overline{f}(s^2T)$. Then modulo the maximal ideal of S,

$$\overline{g}(T) = T^n - \overline{F}T + \overline{\alpha}.$$

Hence $\overline{g}(T) \subseteq R/I[T]$ and the derivative is a nonzero constant. Thus, $\overline{g}$ has n distinct roots and therefore must split over R/I. This contradicts Lemma 20, so our assumption that f is irreducible over S must be false. However, the minimal polynomial for b over S must divide f and using it, we may obtain the same contradiction unless the minimal polynomial is linear. So we have reduced to the case where $b \in S$.

Now we have $z \in (s,u)\overline{S_1[z]}$. Then by Lemma 22, z^3 is a multiple of a cube of an element in the maximal ideal in S_1. Since this was not true in R, this implies that $z^3 \in qR$ for some height one prime q which ramifies under the extension to S_1. By Proposition 13 the only possibilities are $z^3 \in xR$ or $z^3 \in yR$ and the first claim in proved. Without loss of generality, we may assume then that $z^3 \in yR$.

In a similar manner we now show that either $z^3 - vx^2y^2 \in xyI^3$ or $z^3 - vx^2y^2 \in y^2I^3$. Let $\tilde{z} = z/s$. Then $s\tilde{z} \in (u^3, s^3)R^+$ which implies that $\tilde{z} \in (u^3, s^2)R^+$. Also, $\tilde{z}^3 - vu^6s^3 \in (s^3, u^3)^4S_1$ which implies that $\tilde{z}^3 \in (u^2, s^3)^4$. Letting $n = p^2$, note also that $\tilde{z}^{n-1} - F(u^2)^{n-1}s^{n-1} \in ((u^2)^n, s^n)$ where $F = v^{(n-1)/3}$ is a unit. Thus we may now apply Proposition 13 with u^2 in place of x, s in place of y, $c = 3$, $d = e = 1$, and $f = 4$. We obtain $\tilde{z} = u^2a + sb$ where $a, b \in R^+$ and a satisfies $f(T) = T^n + a_1T^{n-1} + \cdots + a_n$ over S_1, an integral extension of S_0. Modulo the integral closure of a fractional power of u, $a_i \equiv 0$ for $i < n-1$ and $a_{n-1} \equiv -Fs^{n-1}$. Since $\tilde{z} \in (u^3, s^2)R^+$, it is easily seen that $a \in (u,s)R^+$. Applying Lemma 20 to the element a gives a contradiction just as above, unless $a \in \overline{S_1[z]}$. But this gives $\tilde{z} \in (s,u)\overline{S_1[\tilde{z}]}$. Then by Lemma 22, $\tilde{z}^3$ is a multiple of a cube of an element in the maximal ideal in S_1. Since this was not true in R, as before this implies that $\tilde{z}^3 \in xR$ or $\tilde{z}^3 \in yR$, as desired.

If $z^3 - vx^2y^2 \in y^2I^3$ let $\tilde{z} = z/s^2$. Then $\tilde{z}^3 - vx^2 \in (x, s^3)^3$. Since $s^2\tilde{z} = z \in (s^3, x)R^+$, we obtain $\tilde{z} \in (x,s)R^+$. But then we must have $x^2 \in (x,s)^3R^+$, which clearly is not true.

If $z^3 - vx^2y^2 \in xyI^3$, let $\tilde{z} = z/su$. Then $\tilde{z}^3 - vs^3u^3 \in (s^3, u^3)^3$. Since $su\tilde{z} = z \in (s^3, u^3)R^+$, we must have $\tilde{z} \in (s^2, u^2)R^+$. But this implies $s^3u^3 \in (s^2, u^2)^3R^+$, also a contradiction. □

Lemma 25. *Let R be a Henselian regular local ring of dimension 2 with maximal ideal $I = (x,y)R$ which has a separably closed residue field and suppose $p > 3$ is a prime with $p \in I$. If $z \in IR^+$, with $z^3 - vy^2x(y + rx) \in yI^4$ where v is a unit of R and $r \in R$, then $z^3 \in y^3R$ or $z^3 \in xR$.*

Proof. The proof is similar to that of Lemma 24. □

Proposition 26. *Let R be a Henselian regular local ring of dimension 2 with maximal ideal $I = (x,y)R$ which has a separably closed residue field and suppose $p > 3$ is a prime with $p \in I$. Suppose $z^3 \in R$, $z \in IR^+$, and $z^3 \notin t^3R$ for any element $t \in I$. Then $z^3 \in t^4R + I^5$ for some element $t \in I$.*

Proof. By Proposition 23, $z^3 \in I^4$. Suppose that

$$z^3 = Ay^4 + By^3x + Cy^2x^2 + Dyx^3 + Ex^4.$$

We shall first show that either the proposition holds or we can reduce to the special case where $A \in I$ and B is a unit. Later we shall show that the special case leads to a contradiction.

Reducing the coefficients modulo I, we consider the polynomial

$$h(T) = \overline{A}T^4 + \overline{B}T^3 + \overline{C}T^2 + \overline{D}T + \overline{E}.$$

First suppose $\overline{A} = \overline{B} = \overline{C} = \overline{D} = 0$. Then the result holds with $t = x$. So we may assume $h(T)$ is not constant and hence that $h(T)$ is a separable polynomial and so splits over the residue field. We consider five possible cases.

Case 1. Suppose $h(T)$ has a quadruple root. Say $h(T) = \overline{A}(T + r)^4$. Then $z^3 \in t^4R + I^5$ with $t = y + rx$.

Case 2. Suppose $h(T)$ is a polynomial of degree 3. Then we must have $A \in I$ and $B \notin I$ which is the special case.

Case 3. Suppose $h(T)$ is a degree two polynomial and there is a double root. In this case, $A, B \in I$ and $C \notin I$, with $h(T) = \overline{C}(T + r)^2$ for some element r. Then $z^3 - Cx^2(y + rx)^2 \in I^5$. Since $(x, y + rx) = I$, by Lemma 24 this is a contradiction.

Case 4. Suppose $h(T)$ is a degree four polynomial and has two double roots. Then it is easily seen that $A \notin I$ and $z^3 - A(y + r_1x)^2(y + r_2x)^2 \in I^5R$, with $r_1 - r_2 \notin I$. Then $I = (y + r_1x, y + r_2x)$ and so Lemma 24 gives a contradiction.

Case 5. Suppose $h(T)$ has a non-multiple root. This is the only remaining possibility. Call this root r. Let $y' = x$ and $x' = y - rx$. Then we get $z^3 = A'(y')^4 + B'(y')^3(x') + \cdots + E'(x')^4$. Because r is a root of $h(T)$, $z^3 \in x'R + I^5$. Because r is not a multiple root, $z^3 \notin (x')^2R + I^5$. This tells us that $A' \in I$ and B' must be a unit which is the special case.

Now we have reduced to the special case where $A \in I$, $B \notin I$. Let $S_0 = R[u]$ where $u^3 = x$. Note that S_0 is a regular local ring with maximal ideal $(u, y)S_0$. Suppose first that $z^3 \in xR$. Then $z^* = z/u$ is integral over S_0. As $z \in IR^+$, we have $uz^* \in (y, u^3)R^+$ and so $z^* \in (y, u^2)R^+$. Since $z^3 \in x^2R$ would contradict the assumption that B is a unit we may apply Proposition 23 to get $(z^*)^3 \in (y, u)^4S_0 \subset (y^4, u)S_0$. However, this is false as $(z^*)^3$ is congruent to By^3 modulo this last ideal and B is a unit. Thus, $z^3 \notin xR$.

Now we have

$$z^3 = Ay^4 + By^3u^3 + Cy^2u^6 + Dyu^9 + Eu^{12}.$$

By changing variables if necessary, we may assume that $z^3 \notin yR$ and still obtain this same equation with $A \in I$ and $B \notin I$. Let $n = p^2$. Then

$$z^{n-1} = Fy^{n-1}u^{n-1} + Hu^n + Gy^n,$$

where to compute F, we raise the expression equal to z^3 to the $(n-1)/3$ power and compute the coefficient of $y^{n-1}u^{n-1}$. This is a sum of terms, one of which is $B^{(n-1)/3}$ and the remaining terms are divisible by A. Since $A \in I$, we see that F is congruent to $B^{(n-1)/3}$ modulo I. Thus we may assume F is a unit. Now we apply Proposition 13 with u in place of x, $c = 3$, $d = 1$, and $f = 4$ to find integral elements v, w such that $z = yv + uw$ where w is a root of $f(T) = T^n + a_1T^{n-1} + \cdots + a_n = 0$ over S_1, an integral extension of S_0. As $yv + uw \in (x, y)R^+$, it quickly follows that $uw \in (x, y)R^+ = (u^3, y)R^+$. From there, we see that $w \in (u^2, y)R^+$. We will apply Lemma 20 with u in place of x.

First, let S denote the integral closure of $S_1[z]$. Suppose that $f(T)$ is irreducible over S. Let P be a height one prime of S containing u. Working modulo P, from the information about the coefficients a_i given in Proposition 13, we observe that $\overline{f}(T) = T^n - \overline{Fy^{n-1}}T + \bar{r}$, where $r \in S_0$. By Lemma 20, the element $\alpha = \overline{r/y^n}$ is integral over S/P. Hence α is in the integral closure of S_0/uS_0. Now S_0/uS_0 is isomorphic to R/xR. Hence, the integral closure of S_0/uS_0 has the same residue field as R since that residue field is separably closed. As in Lemma 20, we let $g(T) = y^{-n}\overline{f}(yT)$. Then modulo the maximal ideal of S, we have $\overline{g}(T) = T^n - \overline{F}T + \overline{\alpha}$. Hence $\overline{g}(T) \subseteq R/I[T]$ and the derivative is a nonzero constant. Thus, $\overline{g}$ has n distinct roots and therefore must split over R/I. This contradicts Lemma 20, so our assumption that f is irreducible over S must be false. However, the minimal polynomial for w over S must divide f and using it, we may obtain the same contradiction unless the minimal polynomial is linear. So we have reduced to the case where $w \in S$.

Since $z = yv + uw$ and S is integrally closed, we obtain $z \in (y, u)S$, so by Lemma 22, z^3 is a multiple of a cube of some element in the maximal ideal of S. Since this was not the case in R, we must have $z^3 \in xR$ or $z^3 \in yR$ since these are the only primes containing z^3 which ramify. This contradiction completes the proof. □

Proposition 28 provides a necessary condition which will be useful in proving Theorem 31 and Proposition 32 below. First, we need a simple lemma.

Lemma 27. *Let R be an integrally closed integral domain. Let $M > 6$ be an integer and let $x, y, t \in R$ with $t^3 = y + x^M$ and $p \in \sqrt{(x, y)R}$. Then $t \in (x, y^{1/3-1/M})R^+$.*

Proof. Let $S = R[s]$ where $s^{3M} = y^{M-3}$. Then

$$t^{3(M-3)} = \left(y + x^M\right)^{M-3} \in \overline{\left(y^{M-3}, x^{M(M-3)}\right)}R \in \overline{\left(s^{3M}, x^{M(M-3)}\right)}S.$$

Since

$$\frac{1}{3M} + \frac{1}{M(M-3)} = \frac{1}{3(M-3)},$$

an application of Corollary 18 gives $t \in (x, s)S^+ = (x, y^{1/3-1/M})R^+$. □

Proposition 28. *Let R be a Henselian regular local ring of dimension two with separably closed residue field and maximal ideal $I = (x, y)R$. Let $p \in I$. Suppose $z^3 \in R$, $z^3 \notin xR$,*

$z^3 \notin y^3R$, and $z^3 = \sum_{(i,j)\in S} u_{i,j}y^i x^j$, where each $u_{i,j}$ is a unit of R. Suppose further that there exists $(a,b) \in S$ with $0 \leqslant a \leqslant 3$, $4-a < b < 3(4-a)$, and $b/(4-a) \leqslant j/(4-i)$ whenever $i \leqslant 3$, $(i,j) \in S$. If there exist $k_1 \leqslant p^2-1$, $k_2 < p^2-1$ with $bk_1 + (4-a)k_2 = 4b((p^2-1)/3)$ such that $z^{p^2-1} - Fy^{k_1}x^{k_2} \in (y^{k_1+1}, x^{k_2+1})$ for some unit F of R, then $z \notin (x,y)R^+$ unless $z^3 \in yR$. Furthermore, if $k_1 < p^2-1$ then for some $M \geqslant p^2-1$, $z \notin (x, y^{1-1/M})R^+$.

Proof. Let $n = p^2$. Let u_1 be an $(n-1)$st root of y, u_2 an $(n-1)$st root of x, and let $S_0 = R[u_1,u_2]$. Note that S_0 is a Henselian regular local ring with a separably closed residue field and maximal ideal $(u_1,u_2)S_0$. Let $t_i = u_i^{k_i}$. Then $y^{k_1} = t_1^{n-1}$, $x^{k_2} = t_2^{n-1}$ and it follows that

$$z^{n-1} - Ft_1^{n-1}t_2^{n-1} \in \left(t_1^n, t_2^n\right)S_0.$$

Let

$$A = \frac{n-1}{k_1} \quad \text{and} \quad B = \frac{n-1}{k_2}\cdot\frac{b}{4-a}.$$

Then $1/A + 1/B = 4/3$ and $p \in (t_1^A, t_2^{Be})$ with $e = (4-a)/b > 1/3$. We may now apply Proposition 13 provided $z^3 \in (t_1^A, t_2^B)^4$. Since $t_1^A = y$, clearly $y^i x^j \in (t_1^A, t_2^B)^4$ if $i \geqslant 4$. If $i < 4$ then $j/(4-i) \geqslant b/(4-a)$ or equivalently, $ej \geqslant (4-i)$. Hence, $y^i x^j = t_1^{Ai} t_2^{Bej} \in (t_1^A, t_2^B)^4$.

We next use Proposition 13 to get $z = t_1 v + t_2 w$ and a degree n polynomial $f(T)$ satisfied by w. The polynomial $f(T)$ is in $S_1[T]$ for some integral extension S_1 of S_0. Assume to the contrary that $z \in (x, y^{1-1/M})R^+$ for every $M \geqslant n-1$. Let $\tilde{y} = y^{1-1/(n-1)}$. Then there exist $\alpha, \beta \in R^+$ with $z = \tilde{y}\alpha + x\beta$. Hence $t_2(w - xt_2^{-1}\beta) = t_1(\tilde{y}t_1^{-1}\alpha - v)$. Since $t_1 = y^{k_1/(n-1)}$ divides $\tilde{y} = y^{(n-2/(n-1)}$ as long as $k_1 < n-1$ and t_2 divides x and no height one prime contains both t_1 and t_2, it follows that $(w - xt_2^{-1}\beta)/t_1 \in R^+$. Thus $w \in (t_1, xt_2^{-1})R^+ \subset (t_1,u_2)R^+$. Similarly, if $z \in IR^+$, then $z = y\alpha + x\beta$ and since $t_1 = y^{k_1/(n-1)}$ divides y whenever $k_1 \leqslant n-1$ we may again obtain $w \in (t_1, xt_2^{-1})R^+ \subset (t_1,u_2)R^+$.

Finally we apply Lemma 20 to the element w with t_1 in place of y and u_2 in place of x. First, let S denote the integral closure of $S_1[z]$ and suppose $f(T) = T^n + a_1T^{n-1} + \cdots + a_n$ is irreducible over S. Let P be a height one prime of S containing u_2. From the technical information about $f(T)$ given in Proposition 13, modulo P we have $a_i \equiv 0$ for $i < n-1$, $a_{n-1} \equiv -Ft_1^{n-1}$, and $a_n \equiv r$ for some $r \in S_0$. Working modulo P we have $\overline{f}(T) = T^n - \overline{Ft_1^{n-1}}T + \overline{r}$. By Lemma 20, the element $\alpha = \overline{r/t_1^n}$ is integral over S/P. Hence α is in the integral closure of S_0/u_2S_0. Now S_0/u_2S_0 is isomorphic to $(R/xR)[u_1]$, a discrete valuation ring with the same residue field as R/xR. Thus, the integral closure of S_0/u_2S_0 has the same residue field as R. As in Lemma 20, we let $g(T) = t_1^{-n}\overline{f}(t_1T)$. Then modulo the maximal ideal of S,

$$\overline{g}(T) = T^n - \overline{F}T + \overline{\alpha}.$$

Hence $\overline{g}(T) \subseteq R/I[T]$ and the derivative is a nonzero constant. Thus, $\overline{g}$ has n distinct roots and therefore must split over R/I. This contradicts Lemma 20, so our assumption that f is irreducible over S must be false. However, the minimal polynomial for w over S must divide f and using it, we may obtain the same contradiction unless the minimal polynomial is linear. So we have reduced to the case where $w \in S$.

Now we have $z \in (t_1, t_2)S \subset (u_1, u_2)S$. By Lemma 22, z^3 must be a multiple of the cube of an element in $(u_1, u_2)S_1$. Since this property did not hold in R and since xR and yR are the only ramified primes in the extension which contain z^3, we must have $z^3 \in xR$ or $z^3 \in yR$. By assumption, $z^3 \notin xR$. We consider two cases.

Case 1. Suppose that $z^3 = yr$, for some $r \in R$, $r \notin yR$ and that $k_1 < n-1$. Recall that we are assuming to the contrary that $z^3 \in (x, y^{1-1/M})R^+$ for all $M \geqslant n-1$. Choose $M = 2(n-1)$. Let $\tilde{z}^3 = z^3 + rx^M$. Since $\tilde{z}^3 \notin yR$, we will show that the above argument can be applied to $\tilde{z}$ to obtain a contradiction. It is easily seen that all of the assumptions on z in the statement of the proposition also hold for $\tilde{z}$ with the same a, b, k_1, and k_2. It remains only to show that $\tilde{z} \in (x, y^{1-1/(n-1)})R^+$ to be able to obtain the contradiction.

Now, $\tilde{z} = r^{1/3}t$, where $t = (y + x^M)^{1/3}$. From Lemma 27 we have $t \in (x, y^{1/3-1/M})R^+$. From the fact that $z \in (x, y^{1-1/M})R^+$, it is easily seen that $r^{1/3} \in (x, y^{2/3-1/M})R^+$. Thus, $\tilde{z} \in (x, y^{1-2/M})R^+ = (x, y^{1-1/(n-1)})R^+$.

Case 2. Suppose that $z^3 = y^2r$, for some $r \in R$, $r \notin yR$ and that $k_1 < n-1$. Now choose $M = 3(n-1)$. Let $\tilde{z}^3 = z^3 + rx^M$. The argument is now similar to that of Case 1. We have $\tilde{z} = r^{1/3}t$, where $t = (y^2 + x^M)^{1/3}$. From Lemma 27 we see that $t \in (x, y^{2/3-2/M})R^+$. As $z \in (x, y^{1-1/M})R^+$, it is easily seen that $r^{1/3} \in (x, y^{1/3-1/M})R^+$. Thus, $\tilde{z} \in (x, y^{1-3/M})R^+ = (x, y^{1-1/(n-1)})R^+$ and so the above argument can be applied to $\tilde{z}$ to obtain a contradiction. □

Notice that the value $\lfloor (p^2-1)/bp \rfloor$ in the statements of the next two lemmas has the simpler representation $\lfloor (p-1)/b \rfloor$. However, the former expression will prove to be more useful when applying these results.

Lemma 29. *Let p, a, b be integers such that $0 \leqslant a \leqslant 3$ and $4-a < b < 3(4-a)$. Use the division algorithm to write $p = 3(4-a)q + r$, with $0 \leqslant r < 3(4-a)$. If $q + r \geqslant 3(4-a)$, then*

$$\frac{p^2-1}{3(4-a)p} \leqslant \left\lfloor \frac{p^2-1}{bp} \right\rfloor.$$

Proof. First, notice that

$$\frac{p^2-1}{3(4-a)p} = q + \frac{rp-1}{3(4-a)p} < q+1.$$

Also,

$$\left\lfloor \frac{p^2-1}{bp} \right\rfloor \geqslant \left\lfloor \frac{p^2-1}{(3(4-a)-1)p} \right\rfloor = \left\lfloor q + \frac{(q+r)p-1}{(3(4-a)-1)p} \right\rfloor.$$

So the result holds if $q + r \geqslant 3(4-a)$. □

Lemma 30. *Let a, b be integers such that $0 \leqslant a \leqslant 3$ and $4 - a < b < 3(4-a)$. Let p be a prime number with $p > 43$. Then with either $k = p\lfloor (p^2-1)/(bp) \rfloor$ or $k = \lceil (p^2-1)/(3(4-a)) \rceil$, the following must hold*:

(1) $\binom{(p^2-1)/3}{k}$ *is not divisible by* p,

(2) $k < \dfrac{p^2-1}{b}$, *and*

(3) $k \geqslant \dfrac{p^2-1}{3(4-a)}$.

In fact, we can choose such a k with $k > (p^2-1)/(3(4-a))$ if $1 \leqslant a \leqslant 3$.

Proof. For convenience, let $k_1 = p\lfloor (p^2-1)/(bp) \rfloor$ and $k_2 = \lceil (p^2-1)/(3(4-a)) \rceil$. Notice that (1) holds for k_1 by Lemma 14. It is obvious that condition (2) holds for k_1 and that (3) holds for k_2. To see that (2) always holds for k_2, note that unless $a = 1$, $3(4-a)$ divides $p^2 - 1$ and certainly

$$\frac{p^2-1}{3(4-a)} < \frac{p^2-1}{b}.$$

If $a = 1$, then since $b \leqslant 8$ it suffices to show that

$$\frac{p^2-1}{9} + 1 < \frac{p^2-1}{8},$$

or equivalently, that $8(p^2-1) + 72 < 9(p^2-1)$. Since $p > 43$ this is certainly true.

Use the division algorithm to write $p = 3(4-a)q + r$ with $0 \leqslant r < 3(4-a)$. By Lemma 29, condition (3) holds for k_1 as long as $q + r \geqslant 3(4-a)$. Hence for $a = 3$ the result is certainly true. If $a = 2$, then $p = 6q + r$ and (3) holds as long as $q + r \geqslant 6$. Since $q \geqslant 7$, there is no problem. If $a = 0$ or $a = 1$, we claim that (1) holds for k_2 if $r = 1, 2$, or 5 and that (3) holds for k_1 otherwise. The verification of this claim is enough to complete the proof of the first statement. This can be checked by applying Lemmas 14 and 29. We leave the details to the reader.

To prove the final statement, note that if $k = p\lfloor (p^2-1)/(bp) \rfloor$, then $k > (p^2-1)/(3(4-a))$ since $(p^2-1)/(3(4-a))$ is not evenly divisible by p. Hence we need only consider the case when $k = \lceil (p^2-1)/(3(4-a)) \rceil$ and $3(4-a) \mid p^2 - 1 = (p-1)(p+1)$.

This is equivalent to requiring that $3(4-a)$ divides $r-1$ or $r+1$. The only cases above in which we are forced to choose $k = \lceil (p^2-1)/(3(4-a)) \rceil$ turn out to be when $a = 1$, $r \in \{1, 2\}$, and $q + r < 9$. Since 9 must divide $r-1$ or $r+1$, we may assume $p = 9q+1$ and $q \leqslant 7$. There are no such primes greater than 43. □

Theorem 31. *Let R be a Henselian regular local ring of dimension two with separably closed residue field and maximal ideal $I = (x, y)R$. Let p be a prime integer with $p \in I$, $p > 43$. Suppose z is integral over R with*

$$z^3 = f(x, y) = y^4 A + \sum_{(i,j)\in S} u_{i,j} y^i x^j \in R, \quad z^3 \notin y^3 R,$$

where A and each $u_{i,j}$ are units and the set S satisfies the following:

(1) *if $(4, j) \in S$, then $j \geqslant 1$ and*
(2) *there is an $(a, b) \in S$ with $0 \leqslant a \leqslant 3$ and $4 - a < b < 3(4-a)$ such that $b/(4-a) < j/(4-i)$ whenever $i < 4$, $(i, j) \in S$, $(i, j) \neq (a, b)$.*

Then $z \notin IR^+$.

Proof. We may obtain a valuation v on the quotient field of R with $v(y) = b$, $v(x) = 4-a$, and with the valuation of any polynomial in x and y equal to the infimum over all monomials. Then $v(y^4 A) = 4b = v(uy^a x^b)$. We claim that $v(z^3) = 4b$ and that only the terms $y^4 A$ and $uy^a x^b$ have the minimum value. If $i \geqslant 4$, then $v(u_{i,j} y^i x^j) = ib + j(4-a) \geqslant 4b$. In fact, by assumption (1), this value is strictly greater than 4b unless the term is $y^4 A$. If $i < 4$ then $b/(4-a) < j/(4-i)$ implies that $b(4-i) < j(4-a)$ or $4b < ib + j(4-a) = v(u_{i,j} y^i x^j)$, thus proving the claim.

Let $n = p^2$. Let $k = p\lfloor (n-1)/(bp) \rfloor$ or $k = \lceil (n-1)/(3(4-a)) \rceil$ depending on which choice satisfies conditions (1)–(3) of Lemma 30. Let $k_1 = 4((n-1)/3) - (4-a)k$ and $k_2 = bk$. Observe that $bk_1 + (4-a)k_2 = 4b((n-1)/3)$. By condition (2) of Lemma 30, $k_2 < n-1$ and by (3), $k_1 \leqslant n-1$.

Certainly, we have $z^{n-1} = [f(x, y)]^{(n-1)/3}$. We first claim that if $y^c x^d$ occurs with unit coefficient in this expression, then either $c \geqslant k_1 + 1$ or $c + d \geqslant k_1 + k_2$. If this is not the case, then since $b \geqslant 4 - a$, we have

$$v\big(y^c x^d\big) = cb + d(4-a) \leqslant k_1 b + (k_2 - 1)(4-a) \leqslant 4b\left(\frac{n-1}{3}\right) - (4-a).$$

But we must also have

$$v\big(y^c x^d\big) \geqslant v\big(z^{n-1}\big) = \left(\frac{n-1}{3}\right) 4b,$$

a contradiction. Thus, $z^{n-1} \subset y^{k_1+1} R + I^{k_1+k_2}$.

Next we claim that there is a term of the form $vy^{k_1}x^{k_2}$ in this expression where v is a unit. In the expansion of $[f(x,y)]^{(n-1)/3}$ we do in fact have the term

$$\binom{(n-1)/3}{k}\left(y^4A\right)^{(n-1)/3-k}\left(uy^ax^b\right)^k=\binom{(n-1)/3}{k}A^{(n-1)/3-k}u^ky^{k_1}x^{k_2}.$$

Since $\binom{(n-1)/3}{k}$ is a unit by Lemma 30, we may take

$$v=\binom{(n-1)/3}{k}A^{(n-1)/3-k}u^k.$$

Note that the term $vy^{k_1}x^{k_2}$ cannot be cancelled out by terms involving the remaining summands of $f(x,y)$ since $vy^{k_1}x^{k_2}$ has the minimum possible value and all terms with minimal value must come from the binomial expansion of $(Ay^4+uy^ax^b)^{(n-1)/3}$. We now have

$$z^{n-1}-vy^{k_1}x^{k_2}\in\left(y^{k_1+1},x^{k_2+1}\right)R$$

and an application of Theorem 28 completes the proof unless $k_1=n-1$ and $z^3\in yR$. In this case, $a\geqslant 1$ and $k=(n-1)/(3(4-a))$, which Lemma 30 assures us can be avoided. □

Finally, we would like to point out what remains to be done to complete the proof of Conjecture 2 if R is a two-dimensional Henselian regular local ring with a separably closed residue field and $I=(x,y)$ is the maximal ideal. We conjecture that if $z\in IR^+$, but $z^3\notin I^5$, then either $z^3\in t^3R$ or $z^3\in(t,I^3)^4R$ for some $t\in I$. This is a weaker version of Conjecture 2 and seems to be a key preliminary step to proving that result. By Proposition 26, we may assume that $z^3=y^4A+\sum_{(i,j)\in S}u_{i,j}y^ix^j$ with A a unit and $j>4-i$ for all $(i,j)\in S$. If $i\geqslant 3$ for all $(i,j)\in S$, then $z^3\in y^3R$. If $j\geqslant 3(4-i)$ for every $(i,j)\in S$ then $z^3\in(y,x^3)^4R$. So to prove this weaker conjecture it remains to prove that $z\notin IR^+$ whenever condition (2) of Theorem 31 fails because there is an $(a,b)\in S$ with $0\leqslant a\leqslant 3$ and $4-a<b<3(4-a)$ such that $b/(4-a)\leqslant j/(4-i)$ whenever $i<4$, $(i,j)\in S$, and equality holds for at least one $(i,j)\neq(a,b)$. This can only happen in the following three situations:

(1) Both $(2,3)$ and $(0,6)$ are in S and $3/2\leqslant j/(4-i)$, for $i<4$.
(2) Both $(2,5)$ and $(0,10)$ are in S and $5/2\leqslant j/(4-i)$, for $i<4$.
(3) Any two of $(3,2)$, $(2,4)$, $(1,6)$, $(0,8)$ are in S and $2\leqslant j/(4-i)$, for $i<4$.

Our next proposition is a significant step towards resolving these three situations and a good illustration of the tools that we have available. Theorem 35 will then fully resolve the first case for $p\equiv 1\pmod 3$.

Proposition 32. *Let R be a Henselian regular local ring of dimension two with separably closed residue field and maximal ideal $I = (x, y)R$. Let p be a prime integer with $p \in I$. Suppose z is integral over R with*

$$z^3 = y^4A + y^2x^bB + x^{2b}C + \sum_{(i,j)\in S} u_{i,j}y^ix^j \in R,$$

where A, B, C are units of R, $3 \leqslant b \leqslant 5$, and $b/2 < j/(4-i)$ for every $(i, j) \in S$, $i < 4$. Let

$$f_k(T) = \sum_{i=k-N}^{\lfloor k/2\rfloor} \binom{N}{i, k-2i, N-k+i} T^i,$$

where $N = (p^2-1)/3$. If AC/B^2 is not a root of $f_k(T)$ modulo the maximal ideal of R for some $((2b-3)/b)N < k \leqslant (3/2)N$, then $z \notin IR^+$.

Proof. We may obtain a valuation v on the quotient field of R with $v(y) = b$, $v(x) = 2$, and with the valuation of any polynomial in x and y equal to the infimum over all monomials. Then

$$v\big(y^4A\big) = v\big(y^2x^bB\big) = v\big(x^{2b}C\big) = 4b.$$

We claim that $v(z^3) = 4b$ and that only the terms y^4A, y^2x^bB, and $x^{2b}C$ have the minimum value. If $i < 4$ then $b/2 < j/(4-i)$ implies that $b(4-i) < 2j$ or $4b < bi + 2j = v(y^ix^j)$, thus proving the claim.

Choose

$$\left(\frac{2b-3}{b}\right)N < k \leqslant \frac{3}{2}N.$$

Let $k_1 = 2k$ and $k_2 = 2bN - bk$. Then $bk_1 + 2k_2 = 4bN$ and it is easy to check that $0 \leqslant k_1 \leqslant p^2 - 1$ and $0 \leqslant k_2 < p^2 - 1$. Certainly,

$$z^{p^2-1} = \left[y^4A + y^2x^bB + x^{2b}C + \sum_{(i,j)\in S} u_{i,j}y^ix^j\right]^N.$$

We first claim that if y^cx^d occurs with unit coefficient in this expression, then either $c \geqslant k_1 + 1$ or $c + d \geqslant k_1 + k_2$. If this is not the case, then

$$v\big(y^cx^d\big) = bc + 2d \leqslant (b-2)k_1 + 2(k_1 + k_2 - 1) = bk_1 + 2k_2 - 2 = 4bN - 2.$$

But we must also have $v(y^cx^d) \geqslant v(z^{p^2-1}) = 4bN$, a contradiction. Thus,

$$z^{p^2-1} - Fy^{k_1}x^{k_2} \subseteq \big(y^{k_1+1}, x^{k_2+1}\big),$$

for some $F \in R$.

By Proposition 28, we now only need to show that F is a unit if $f_k(AC/B^2)$ is not congruent to zero modulo the maximal ideal of R. Since $v(y^{k_1}x^{k_2}) = bk_1 + 2k_2 = 4bN$ is the minimum possible value for a term in the expansion of z^{p^2-1}, the only possible terms contributing to F are those of the form

$$\binom{N}{i, k-2i, N-k+i} A^i B^{k-2i} C^{N-k+i} y^{k_1} x^{k_2}.$$

Thus we may take F to be

$$B^k C^{N-k} f_k\left(\frac{AC}{B^2}\right)$$

which completes the proof. □

Notice that for $p \equiv 1 \pmod 3$ we may write $p = 6q + 1$. It can be shown (by reducing modulo the maximal ideal and by dividing through by the smallest power of T) that the polynomials of Proposition 32 may then be replaced with the polynomials

$$f_l(T) = \sum_{i=0}^{2q-\lceil l/2 \rceil} \binom{2q}{i, i+l-2q, 4q-l-2i} T^i,$$

for $2q + 1 \leqslant l \leqslant 3q$ when $b = 3$. These polynomials will be used in what follows.

Lemma 33. *Let M be a maximal ideal of R and let f and g be polynomials over R with $f = \sum_0^n c_i T^i$ and $g = \sum_0^n (1/(i+k)) c_i T^i$ for some integer $k \geqslant 1$. If α is a unit of R and is a root of both f and g modulo M, then α is a double root modulo M of g.*

Proof. Since

$$kg = f - \sum_0^n \frac{i}{i+k} c_i T^i = f - Tg',$$

it follows that α is a root of g' and hence a double root of g modulo M. □

Lemma 34. *Let l, q be positive integers with $l \leqslant 4q$. Let*

$$c_{i,l} = \binom{2q}{i, i+l-2q, 4q-l-2i}$$

for $0 \leqslant i \leqslant 2q - \lceil l/2 \rceil$ and $c_{i,l} = 0$, otherwise. Then

$$c_{i,l+1} = -2c_{i,l} + (l+2)\frac{c_{i,l}}{i+l-2q+1} \quad \text{for all } i \geqslant 0.$$

Proof. For $0 \leqslant i \leqslant 2q - \lceil (l+1)/2 \rceil$, simply observe that

$$c_{i,l+1} = \left(\frac{4q - l - 2i}{i + l - 2q + 1} \right) c_{i,l} = \left(-2 + \frac{l+2}{i+l-2q+1} \right) c_{i,l}.$$

If

$$2q - \left\lceil \frac{l}{2} \right\rceil = 2q - \left\lceil \frac{l+1}{2} \right\rceil$$

we are done. It remains only to show the equality when l is even, say $l = 2y$ and $i = 2q - y$. In this case,

$$-2c_{i,l} + (2y+2)\frac{c_{i,l}}{y+1} = \left(-2 + \frac{2y+2}{y+1} \right) c_{i,l} = 0. \qquad \square$$

Theorem 35. *Let R be a Henselian regular local ring of dimension two with separably closed residue field and maximal ideal $I = (x, y)R$. Let p be a prime integer with $p \in I$ and $p \equiv 1 \pmod 3$. Suppose z is integral over R with*

$$z^3 = y^4 A + y^2 x^3 B + x^6 C + \sum_{(i,j) \in S} u_{i,j} y^i x^j \in R,$$

where A, B, C are units of R and $3/2 < j/(4-i)$ for every $(i, j) \in S$, $i < 4$. Then $z \notin IR^+$.

Proof. Write $p = 6q + 1$. From Proposition 32 and the remarks following, it suffices to prove that for $2q + 1 \leqslant l \leqslant 3q$ the polynomials $f_l(T) = \sum_0^{2q - \lceil l/2 \rceil} c_{i,l} T^i$, where $c_{i,l}$ is as in Lemma 34, have no common root. Suppose to the contrary that α is a root of $f_{2q+1}, f_{2q+2}, \ldots, f_{3q}$ modulo M. For $k \geqslant 1$ let

$$f_l^k(T) = \sum_{i=0}^{q - \lceil l/2 \rceil} d_{i,l}^k T^i,$$

with

$$d_{i,l}^k = \frac{c_{i,l}}{(i+l-2q+1)(i+l-2q+2)\cdots(i+l-2q+k)}.$$

Then, applying Lemma 34, we have

$$\begin{aligned} f_{l+1}(T) &= \sum_{i=0}^{q - \lceil (l+1)/2 \rceil} c_{i,l+1} T^i = -2 \sum_{i=0}^{q - \lceil l/2 \rceil} c_{i,l} T^i + (l+2) \sum_{i=0}^{q - \lceil l/2 \rceil} \frac{c_{i,l}}{(i+l-2q+1)} T^i \\ &= -2 f_l(T) + (l+2) f_l^1(T). \end{aligned}$$

From this we see that α is a root of $f_l^1(T)$ modulo M for each $2q+1 \leqslant l \leqslant 3q-1$. Similarly, one can check that

$$f_{l+1}^k(T) = -2f_l^k(T) + (2k+l+2)f_l^{k+1}(T).$$

Notice that for $0 \leqslant k \leqslant q-2$ the element $2k+l+2 \leqslant 5q-2 < p$ and so it is a unit of R. Hence α is a root of f_l^{k+1} modulo M for $0 \leqslant k \leqslant q-2$ and for $2q+1 \leqslant l \leqslant 3q-k-1$.

We claim that α is a root of multiplicity $k+1$ of f_l^k modulo M. First, note that since the ith term of f_l^1 is $1/(i+l-2q+1)$ times the ith term of f_l, Lemma 33 shows that α is a root of multiplicity at least two of f_l^1 modulo M for $2q+1 \leqslant l \leqslant 3q-1$. In addition, since each term of the nth derivative of f_l^{k+1} is simply $1/(i+l-2q+k+1)$ times the corresponding term of the nth derivative of f_l^k, by Lemma 33 it follows that if α is a root of multiplicity $k+1$ modulo M of f_l^k then it is a root of multiplicity $k+2$ modulo M of f_l^{k+1}.

We have shown that f_{2q+1}^{q-1} has a root of multiplicity q modulo M. However, the degree of this polynomial is the same as that of f_1 which is $q - \lceil 1/2 \rceil = q-1$. This is a contradiction. □

Unfortunately, the technique used to prove Theorem 35 does not work when the b of Proposition 32 is equal to 4 or 5. In those cases, although a similar proof would show that a certain polynomial would have a multiple root, unfortunately the degree of the polynomial is much greater than the multiplicity of the root. A new approach is needed to attack these remaining cases.

Acknowledgments

I thank Raymond Heitmann and the referee for their careful reading of this manuscript and their helpful suggestions.

References

[1] R. Heitmann, The plus closure in mixed characteristic, J. Algebra 193 (1997) 688–708, doi:10.1006/jabr.1997.7023.
[2] R. Heitmann, The plus closure in degree two extensions, J. Algebra 218 (1999) 621–641, doi:10.1006/jabr.1999.7914.
[3] M. Hochster, C. Huneke, Tight closure, invariant theory, and the Briançon–Skoda theorem, J. Amer. Math. Soc. 3 (1990) 31–116.
[4] S. Lang, Algebra, Addison–Wesley, Menlo Park, CA, 1993.
[5] O. Zariski, P. Samuel, Commutative Algebra, vols. I, II, Van Nostrand, Princeton, NJ, 1958–1960.